

October 20, 2016

Tom Wheeler
Chairman

Mignon Clyburn
Commissioner

Michael O’Rielly
Commissioner

Ajit Pai
Commissioner

Jessica Rosenworcel
Commissioner

Federal Communications Commission
445 12th Street SW
Washington, D.C. 20554

Re: WC Docket No. 16-106, *Protecting the
Privacy of Customers of Broadband and
Other Telecommunications Services*

Dear Chairman Wheeler and Commissioners:

As you approach the date to vote on a final order in the above-referenced proceeding, American Civil Liberties Union, Benton Foundation,¹ Center for Democracy & Technology, Center for Digital Democracy, Color Of Change, Consumer Action, Consumer Federation of America, Electronic Frontier Foundation, Free Press, New America’s Open Technology Institute, and Public Knowledge urge you to take a strong stance on broadband privacy and to improve the current proposal in modest ways.

In particular, the Commission must not to yield to calls from CTIA,² TechFreedom,³ T-Mobile,⁴ AT&T,⁵ and others to severely limit the scope of covered “sensitive” information, nor otherwise weaken the privacy proposal as outlined in the fact sheet.

¹ The Benton Foundation is a nonprofit organization dedicated to promoting communication in the public interest. These comments reflect the institutional view of the Foundation and, unless obvious from the text, are not intended to reflect the views of individual Foundation officers, directors, or advisors.

² CTIA Notice of Ex Parte, WC Docket No. 16-106 (filed Oct. 17, 2016).

³ TechFreedom Notice of Ex Parte, WC Docket No. 16-106 (filed Oct. 18, 2016).

⁴ T-Mobile Presentation, WC Docket No. 16-106 (filed Oct. 14, 2016).

⁵ AT&T Notice of Ex Parte, WC Docket No. 16-106 (filed Oct. 17, 2016).

With respect to this sensitive information determination, there are clear statutory requirements and policy rationales for setting the privacy obligations of telecommunications providers apart from and above the privacy obligations of other kinds of companies across the economy. The FCC has a mandate to protect the privacy of broadband ISP customers, and to comply with that mandate it should adopt rules that require opt-in consent to share all web-browsing history, app usage, IP addresses, and MAC addresses.

Telecommunications Privacy Is Important

As Title II of the Communications Act recognizes, network access providers have a heightened obligation to protect consumer privacy. The higher standard for telecommunications carriers derives from the special role of network access. Broadband access in particular is increasingly necessary for finding gainful employment, education, access to housing, and full participation in economic and civic life. It is in society's best interest for people to use network access not only for these vitally important activities, but also as a trustworthy platform for free and unfettered First Amendment activities, including association, political speech, reading and learning, and the expression of all viewpoints, including those that are unpopular, dissenting, or held by a minority of people.

Protecting the privacy, openness, and security of broadband is also of central importance to democracy and social movements. Hundreds of years ago, geography strictly limited the development and expansion of communities. Friendships, coalitions, and associations rose up and grew on a local basis – as many do today. But today, thanks to the power of the internet, not only do we build communities in cities and neighborhoods; we also build communities that leap across deserts and oceans, that cross borders and aren't defeated by time zone shifts and language barriers. It is difficult to imagine Occupy Wall Street, Black Lives Matter, or the Arab Spring without the power of the internet.

To protect and uphold the internet as this crucially important platform for both expression, association, and economic activities, we must minimize privacy concerns by ensuring that network access providers are subject to the highest privacy obligations, as the law requires. Privacy concerns can chill both adoption and use of the internet. As a 2010 FCC survey found, 57% of Internet non-

adopters felt online activities made it too easy for theft of personal information.⁶ The FCC concluded in the *National Broadband Plan* that concerns about online privacy and security “may limit [consumers’] adoption or use of broadband.”⁷ More recently, NTIA reported that 45% of households limited their online activities because of privacy and security concerns.⁸ And in January, focus groups examining adoption challenges in Portland, Oregon universally raised privacy concerns.⁹

We want people to get connected, and we want them to use the internet without fear that the things they do and say online will be shared, sold, and exploited without their knowledge or otherwise used against them. In no event should people have to choose between protecting privacy and getting online.

Telecommunications Providers Have Special Insight into Our Private Lives

Broadband privacy is also of particular importance because, as gatekeepers to the network, telecommunications providers are uniquely positioned to gain insight into the private lives and communications of their customers. In the words of former FCC Commissioner Michael Copps, ISPs “collect extensive information about all of their customers, including location, web browsing and app use history, when and with whom they communicate,

⁶ This number was reported in contrast to 39% of adopters who felt the same way. John Horrigan, *Broadband Adoption and Use in America* 17 (FCC Nat’l Broadband Plan, Working Paper No. 1, 2010), <https://transition.fcc.gov/DiversityFAC/032410/consumer-survey-horrigan.pdf>.

⁷ FCC, *Connecting America: The National Broadband Plan* 17 (2010), <https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf>.

⁸ Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NTIA (May 13, 2016), <https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>.

⁹ Angela Siefer, *Signs On Letter Encouraging FCC Protect Privacy Of Broadband Consumers*, NDIA (Jan. 26, 2016), <http://www.digitalinclusionalliance.org/blog/2016/1/26/ndia-signs-on-letter-encouraging-fcc-protect-privacy-of-broadband-consumers>.

and even the content of those communications.”¹⁰ He noted, “In short, nearly everything a consumer does online is visible to his or her ISP.”¹¹

Indeed, consumers have no choice but to share intimate details about their most private activities with their ISP. Just as we have to tell the postal service who we write to, when, and how often—just as we have to tell phone companies similar details about our calls—we have to tell ISPs where we go, what we say, and what we read online so they know how to direct Internet traffic. This is of particular concern as the Internet of Things expands, and data regarding network use may reveal information about the types of connected devices consumers have in their homes, and when, how often, and how much those devices are used.¹²

Nor does the growth of encryption protect consumers’ online activities from their ISPs. Truly pervasive encryption may never happen, and even if it does, it is still a long way off.¹³ Moreover, as privacy law expert Paul Ohm recently testified before Congress:

Even for user visits to websites that deploy encryption, a BIAS provider retains a significant ability to observe. When you visit a website protected by the most widespread form of encryption in use, https or http over TLS, even though your BIAS provider cannot tell which individual page you are visiting on the website, it still can tell the domain name of the website you are communicating with, how often you return, roughly how much data you send and receive, and for how long each visit lasts.¹⁴

¹⁰ Michael Copps, *Consumers Deserve More Privacy Protections, Not Less*, Medium (Oct. 19, 2016), <https://medium.com/@coppsm/consumers-deserve-more-privacy-protections-not-less-ec487a032925>.

¹¹ *Id.*

¹² OTI Notice of Ex Parte, WC Docket No. 16-106 (filed Oct. 13, 2016).

¹³ See generally Upturn, *What ISPs Can See: Clarifying the Technical Landscape of the Broadband Privacy Debate* (2016), <https://www.teamupturn.com/reports/2016/what-isps-can-see>.

¹⁴ *FCC Overreach: Examining the Proposed Privacy Rules: Hearing Before the Subcomm. on Commc’ns and Tech. of the H. Comm. on Energy and Commerce, 114th Cong. 52* (2016) (testimony of Paul Ohm, Prof., Georgetown University Law

Despite ISPs downplaying the window they have into their customers' online activities, there is no question that they are well-positioned to learn a great deal about their customers' lives.

The FCC Should Not Replicate the FTC's Approach

The heightened privacy obligations set forth by Congress in Title II of the Communications Act establish the legal basis, just as the importance of network access and unique nature of network providers' insight into private lives establish the policy basis, for the FCC to promulgate strong privacy rules for broadband providers. In recent weeks, however, a number of industry commenters appear to have fundamentally misunderstood or underestimated the justifications for strong broadband privacy rules. Several do not seem to understand that these justifications mandate a stronger broadband privacy framework than the general privacy protections enforced by the FTC for the rest of the online ecosystem. For example, TechFreedom suggests that "the FCC follow the FTC's substantive approach" and interpret the FCC's various authorities under the Communications Act similarly to how the FTC has interpreted its § 5 authority.¹⁵ The Future of Privacy Forum asserts, "the FCC has an opportunity to make distinctions that reinforce the FTC's standards."

But the Communications Act and the FTC Act protect privacy in different ways and for different reasons. As privacy advocates have previously written,¹⁶ quite obviously the FCC is not the FTC, the Communications Act is not the FTC Act, and § 222 of the Communications Act is not § 5 of the FTCA. In contrast to the heightened and specific privacy protections set forth in § 222, the FTC's privacy approach stems from its broad consumer protection authority and its general mandate. In the FTC's own words, "no other federal agency has the FTC's breadth of authority to protect consumers from many unfair or deceptive

Center) *available at* <http://docs.house.gov/meetings/IF/IF16/20160614/105057/HHRG-114-IF16-Wstate-OhmP-20160614-U1.pdf>.

¹⁵ TechFreedom Notice of Ex Parte, *supra* note 3.

¹⁶ Privacy Advocates' letter to Tom Wheeler, Chairman, Federal Communications Commission, *et al.* WC Docket No. 16-106 (filed Sept. 28, 2016).

practices across the economy and to obtain redress for consumer harm.”¹⁷ In contrast, the task before the FCC is not to set a baseline for all consumer privacy across the entire information ecosystem, but to enact strong and specific privacy protections for telecommunications customers.

Therefore the idea that the FCC should “follow” or “reinforce” the FTC’s privacy approach makes no sense, and the FCC should not do so.

Conclusion

The below-signed organizations appreciate the hard work this Commission has done and is doing to protect consumer privacy. We urge you to vote next week to pass strong broadband privacy rules, and not to yield to industry calls to weaken the proposal. The legal and policy reasons for heightened consumer privacy protections for telecommunications customers are clear.

Sincerely,

American Civil Liberties Union
Benton Foundation
Center for Democracy & Technology
Center for Digital Democracy
Color Of Change
Consumer Action
Consumer Federation of America
Electronic Frontier Foundation
Free Press
New America’s Open Technology
Institute
Public Knowledge

¹⁷ Petition of the Fed. Trade Comm’n for Rehearing *En Banc* 7-8, *Fed. Trade Comm’n v. AT&T Mobility LLC*, No. 15-16585 (9th Cir. Oct. 13, 2016).